

DOCKET NO.: 274883US2PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Bernard LE BARS, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HEREWITH

INTERNATIONAL APPLICATION NO.: PCT/FR03/50161

INTERNATIONAL FILING DATE: December 11, 2003

FOR: METHOD FOR DISTRIBUTING SCRAMBLED SERVICES AND/OR DATA

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119**  
**AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents  
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

**COUNTRY**  
France

**APPLICATION NO**  
02 15736

**DAY/MONTH/YEAR**  
12 December 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/FR03/50161.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Marvin J. Spivak  
Attorney of Record  
Registration No. 24,913  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

**BEST AVAILABLE COPY**

REC'D 09 MAR 2004

WIPO PCT

# BREVET D'INVENTION

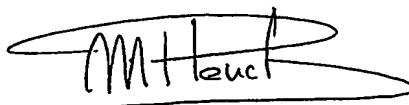
CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 29 DEC. 2003

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets



Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr



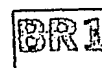
26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08  
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



## REQUÊTE EN DÉLIVRANCE page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DB 510 C W / 210502

<b>REMISE DES PIÈCES</b> DATE <b>12 DEC 2002</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT <b>0215736</b> NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI <b>12 DEC. 2002</b>		<b>1</b> NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE  <b>BREVALEX</b>  <b>3, rue du Docteur Lancereaux</b> <b>75008 PARIS</b>	
<b>Vos références pour ce dossier (facultatif)</b> SP 21819 HM.			
<b>Confirmation d'un dépôt par télécopie</b>		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
<b>2</b> NATURE DE LA DEMANDE Demande de brevet <input checked="" type="checkbox"/> Demande de certificat d'utilité <input type="checkbox"/>  Demande divisionnaire <input type="checkbox"/> <i>Demande de brevet initiale</i> N° _____ Date _____ <i>ou demande de certificat d'utilité initiale</i> N° _____ Date _____ Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i> <input type="checkbox"/> N° _____ Date _____		<b>Cochez l'une des 4 cases suivantes</b> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
<b>3</b> TITRE DE L'INVENTION (200 caractères ou espaces maximum)  <b>PROCEDE DE DISTRIBUTION DE DONNEES ET/OU SERVICES EMBROUILLES</b>			
<b>4</b> DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
<b>5</b> DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale Prénoms Forme juridique N° SIREN Code APE-NAF  Domicile ou siège  Nationalité N° de téléphone (facultatif) Adresse électronique (facultatif)		VIACCESS  Société anonyme _____ _____ Les Collines de l'Arche - Tour Opéra C  <b>92 057</b> PARIS LA DEFENSE CEDEX  FRANCE française  N° de télécopie (facultatif) _____  <input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»	

Remplir impérativement la 2<sup>ème</sup> page

REMISE D'ÉTAT DE DÉCISION 2002  
DATE 75 INPI PARIS  
LIEU 0215736  
N° D'ENREGISTREMENT  
NATIONAL ATTRIBUÉ PAR L'INPI

DB 540 W / 21C532

<b>6 MANDATAIRE (s'il y a lieu)</b>		DU BOISBAUDRY Dominique BREVALEX	
Nom			
Prénom			
Cabinet ou Société			
N° de pouvoir permanent et/ou de lien contractuel			
Adresse	Rue	3, rue du Docteur Lancereaux	
	Code postal et ville	75 008 PARIS	
	Pays	FRANCE	
N° de téléphone (facultatif)		01 53 83 94 00	
N° de télécopie (facultatif)		01 45 63 83 33	
Adresse électronique (facultatif)		brevets.patents@brevaalex.com	
<b>7 INVENTEUR (S)</b>		Les inventeurs sont nécessairement des personnes physiques	
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
<b>8 RAPPORT DE RECHERCHE</b>		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paieement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non	
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG	
<b>10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS</b>		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
Le support électronique de données est joint		<input type="checkbox"/>	
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/>	
Si vous avez utilisé l'imprimé « Suite », indiquez le nombre de pages jointes			
<b>11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)</b>		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>	
D. DU BOISBAUDRY CPI 950304		L. MARTELLO	

PROCEDE DE DISTRIBUTION DE DONNEES ET/OU SERVICES  
EMBROUILLES

DESCRIPTION

5    DOMAINE TECHNIQUE

..... L'invention se situe dans le domaine de la  
distribution sécurisée de données et/ou services dans  
un réseau. ....

Plus spécifiquement, l'invention concerne  
10 un procédé de distribution de données et/ou services  
embrouillés à au moins un terminal maître et à au moins  
un terminal esclave associé audit terminal maître.

L'invention concerne également un système  
de distribution de données et/ou services embrouillés  
15 comportant un module central de gestion des abonnés, un  
générateur de messages de gestion de titres d'accès  
(EMM), une plate-forme d'embrouillage.

Les données et/ou services sont distribués  
à au moins un terminal maître et à au moins un terminal  
20 esclave munis chacun d'un processeur de sécurité. Les  
terminaux maîtres et esclaves pouvant être des  
ordinateurs ou des récepteurs audiovisuels munis d'un  
décodeur. Les processeurs de sécurité sont des  
logiciels enregistrés dans la mémoire de l'ordinateur  
25 ou dans la mémoire d'une carte à puce.

ETAT DE LA TECHNIQUE ANTERIEURE

Lorsqu'un abonné dispose de plusieurs  
terminaux de réception de données et/ou services  
embrouillés, hormis une connexion physique entre les  
30 différents terminaux ou l'utilisation de la voie de

~~retour (identification du N° de Tel appelant ou adresse~~  
MAC (pour Medium Access Control) ou @IP (pour Internet  
Protocol) de chaque terminal, l'opérateur ne dispose  
pas de solution simple lui permettant de contrôler  
5 l'attribution de droits d'accès interdépendants aux  
différents terminaux de l'abonné.

~~Le but de l'invention est de fournir aux~~  
~~opérateurs un procédé et système simples pour affecter~~  
~~de façon contrôlée des droits d'accès interdépendants~~  
10 aux différents terminaux de l'abonné.

#### EXPOSÉ DE L'INVENTION

L'invention préconise un procédé de  
distribution de données et/ou services embrouillés à un  
15 abonné muni d'un terminal maître auquel sont associés  
des droits d'accès principaux et de terminaux  
additionnels esclaves, auxquels sont associés des  
droits d'accès subsidiaires dépendant des droits  
d'accès principaux.

20 Le procédé selon l'invention comporte les  
étapes suivantes :

- transmettre au terminal maître un premier  
code secret  $S_M$  et à chaque terminal esclave un deuxième  
code secret  $S_s$  en relation biunivoque avec le premier  
25 code  $S_M$ ,

- autoriser la réception des données et/ou  
services par un terminal esclave uniquement si le  
premier code secret  $S_M$  est préalablement enregistré  
dans ledit terminal esclave.

30 Ainsi, un abonné peut recevoir les données  
et/ou services sur un terminal principal pour lequel il

a préalablement acquis des droits d'accès et tout ou partie de ces données et/ou services sur plusieurs autres terminaux secondaires pour lesquels il a acquis un droit d'accès associé au droit principal, identique à celui-ci ou restreint par rapport à celui-ci et défini en fonction de choix commerciaux ou de critères spécifiques à chaque terminal (récepteur comportant une limitation parentale, linguistique, etc.).

Par exemple, l'opérateur peut attribuer une réduction de coût à un abonné pour un deuxième abonnement sous réserve que cet abonnement soit effectivement utilisé par ce seul abonné sur son deuxième terminal. De cette façon, l'opérateur peut se prémunir du détournement de cette stratégie commerciale si l'usage du deuxième abonnement était techniquement limité au deuxième terminal de l'abonné.

Dans un mode préféré de réalisation de l'invention, le procédé selon l'invention comporte les étapes suivantes :

- définir un premier type de messages de gestion de titres d'accès (EMMm) pour transmettre le premier code secret  $S_M$  au terminal maître, et un deuxième type de messages de gestion de titres d'accès (EMMs) pour transmettre le deuxième code secret  $S_s$  à chaque terminal esclave,

- enregistrer le premier code secret  $S_M$  dans le terminal maître et le deuxième code secret  $S_s$  dans chaque terminal esclave et à chaque utilisation d'un terminal esclave,

- requérir l'enregistrement du premier code secret  $S_M$  dans ledit terminal esclave si ce deuxième

---

code  $S_s$  n'est pas en relation biunivoque avec le code secret  $S_M$  enregistré dans le terminal esclave.

Avantageusement, le procédé selon l'invention comporte en outre une étape consistant à  
5 générer à fréquence variable un nouveau code secret  $S_M$  et un nouveau code  $S_s$  en relation biunivoque avec le nouveau code  $S_M$ .

---

Dans ce cas, le procédé comporte les étapes suivantes :

10 - définir un premier type de messages de gestion de titres d'accès (EMMm) pour transmettre le nouveau code secret  $S_M$  au terminal maître, et un deuxième type de messages de gestion de titres d'accès (EMMs) pour transmettre le nouveau code secret  $S_s$  à  
15 chaque terminal esclave,

- enregistrer ce nouveau code secret  $S_M$  dans le terminal maître et le nouveau code secret  $S_s$  dans chaque terminal esclave et,

à chaque utilisation d'un terminal esclave,  
20 - si ce nouveau code secret  $S_s$  n'est pas en relation biunivoque avec le code secret  $S_M$  préalablement enregistré dans le terminal esclave,

- requérir l'enregistrement du nouveau code secret  $S_M$  dans ledit terminal esclave.

25

Dans un mode particulier de réalisation, chaque terminal est associé à une carte à puce.

Dans une variante de réalisation, cette carte à puce peut être appariée au terminal.

30 Le procédé selon l'invention est mis en œuvre par un système de distribution de données et/ou

---



services embrouillés comportant un module central de gestion des abonnés, un générateur de messages de gestion de titres d'accès (EMM) et une plate-forme d'embrouillage.

5 Selon l'invention, ce système comporte en outre :

- des moyens pour attribuer au terminal maître un premier code secret  $S_M$ , et à chaque terminal esclave un deuxième code secret  $S_s$  en relation biunivoque avec le premier code secret  $S_M$ ,

- des moyens de contrôle destinés à autoriser la réception des données et/ou services par un terminal esclave uniquement si le premier code secret  $S_M$  est préalablement enregistré dans ledit terminal esclave.

Dans une première variante de réalisation, le système selon l'invention comporte un seul terminal maître et un seul terminal esclave.

Dans une deuxième variante, le système selon l'invention comporte une pluralité de terminaux maîtres, et une pluralité de terminaux esclaves.

#### BREVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif, en référence aux figures annexées dans lesquelles :

- la figure 1 représente un schéma d'un système mettant en œuvre le procédé selon l'invention,  
- la figure 2 représente schématiquement le fonctionnement du système de la figure 1.

---

## EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

---

Afin d'illustrer le procédé selon l'invention, la description qui suit se situe dans un contexte de diffusion de programmes audiovisuels embrouillés à des abonnés connectés à un réseau de télévision numérique.

La figure 1 illustre schématiquement un premier groupe de terminaux 2, 4 d'un premier abonné et un deuxième groupe de terminaux 6, 8 d'un deuxième abonné connectés, via un réseau de transport 10, à un système de diffusion 12.

Ce système de diffusion comporte un module central 14 de gestion des abonnés, un générateur de codes secrets 16 et un générateur de messages de gestion de titres d'accès EMM 18 destinés à véhiculer les codes secrets générés, et une plate-forme d'embrouillage 20.

Les terminaux 2, 4, 6 et 8 sont associés, voire appariés, à une carte à puce 22, 24, 26 et 28 respectivement.

Le générateur de codes secrets 16 comporte un module de calcul apte à définir un premier code secret  $S_{M1}$  et un deuxième code secret  $S_{M2}$ , et à calculer un troisième code secret  $S_{s1}$  en fonction du premier code secret  $S_{M1}$  et un quatrième code secret  $S_{s2}$  en fonction du deuxième code secret  $S_{M2}$ .

Le module central 14 de gestion des abonnés comporte une base de données contenant des informations sur chaque abonné. Ces informations concernent par exemple le nombre de terminaux déclarés par l'abonné et les critères associés à chaque terminal, tel que par

---

exemple les droits d'accès déjà acquis ou des limitations relatives au type de programmes que peut recevoir un terminal ou encore aux plages horaires de réception.

5 Le générateur d'EMM 18 comporte un module logiciel apte à générer des messages EMM(@22,  $S_{M1}$ ), EMM(@24,  $S_{S1}$ ), EMM(@26,  $S_{M2}$ ) et EMM(@28,  $S_{S2}$ ) destinés à véhiculer les codes secrets  $S_{M1}$ ,  $S_{M2}$ ,  $S_{S1}$  et  $S_{S2}$  et les critères de réception définis par le module 14  
10 respectivement au terminal 2, terminal 4, terminal 6 et terminal 8 à travers le réseau de transport 10.

Les messages EMM(@22,  $S_{M1}$ ), EMM(@24,  $S_{S1}$ ), EMM(@26,  $S_{M2}$ ) et EMM(@28,  $S_{S2}$ ) sont transmis de façon répétée aux terminaux de l'abonné.

15 A réception de ces messages EMM, les codes secrets  $S_{M1}$ ,  $S_{M2}$ ,  $S_{S1}$  et  $S_{S2}$  et les critères de réception définis par le module 14 sont inscrits dans les cartes à puce 22, 24, 26 et 28 respectivement. Ces cartes à puce et ou les terminaux comportent un logiciel apte à  
20 distinguer les codes secrets maîtres des codes secrets esclaves.

Les figures 2a à 2c illustrent schématiquement trois situations distinctes dans lesquelles des programmes audiovisuels embrouillés sont  
25 transmis à un abonné muni d'un terminal maître A associé à une carte à puce 30 et de trois terminaux esclaves B, C et D associés respectivement à des cartes à puce 32, 34 et 36.

Dans le cas illustré par la figure 2a, les  
30 programmes embrouillés sont reçus par le terminal maître A où ils sont désembrouillés de façon classique

au moyen d'un mot de contrôle transmis sous forme  
 chiffré dans un message de contrôle de titre d'accès  
 ECM (pour Entitlement Control Message). Le message ECM  
 est exploité dans le terminal A après avoir été  
 5 déchiffré par une clé utilisateur préalablement  
 inscrite dans la carte à puce 30. L'ECM conditionnant  
 l'accès aux programmes est exploitable par le terminal  
 maître A du fait que la carte à puce qui lui est  
 associée dispose d'un code secret maître identique à  
 10 celui qui est stocké dans le terminal maître A. Ainsi,  
 le contrôle des codes secrets de la carte et du  
 terminal peut être effectué indifféremment par la carte  
 ou par le terminal.

Lorsque le contrôle est fait dans la carte,  
 15 si les codes secrets  $S_M$  et  $S_S$  sont en relation  
 biunivoque, celle-ci envoie un ECM déchiffré  
 exploitable au terminal, sinon, elle n'envoie pas un  
 tel ECM au terminal.

Par contre, si le contrôle est effectué  
 20 dans le terminal, la carte à puce envoie un ECM  
 déchiffré et le terminal accepte ou n'accepte pas  
 d'exploiter cet ECM selon que les codes secrets  $S_M$  et  $S_S$   
 sont en relation biunivoque ou ne le sont pas.

25 Dans le cas illustré par la figure 2a, la  
 carte à puce 32 du terminal esclave B comporte un code  
 secret  $S_{S1}$  en relation biunivoque avec le code secret  
 $S_{M1}$  préalablement enregistré (flèche 38) dans le  
 terminal esclave B au moyen de la carte à puce 30.

30 Les programmes embrouillés sont reçus par  
 le terminal esclave B où ils sont désembrouillés de

façon classique au moyen d'un mot de contrôle transmis sous forme chiffré dans un message de contrôle de titre d'accès ECM (pour Entitlement Control Message). Le message ECM est exploité dans le terminal B après avoir  
 5 été déchiffré par une clé utilisateur préalablement inscrite dans la carte à puce 32. L'ECM conditionnant l'accès aux programmes est exploitable par le terminal  
 esclave B du fait que la carte à puce qui lui est associée dispose d'un code secret esclave correspondant  
 10 de manière biunivoque au code secret maître stocké dans le terminal maître B.

Ainsi, dans ce cas également, le contrôle des codes secrets de la carte et du terminal peut être effectué indifféremment par la carte ou par le  
 15 terminal.

Dans le cas illustré par la figure 2b, le code secret  $S_{M1}$  n'a pas encore été transféré dans le terminal esclave C. Les programmes embrouillés reçus  
 20 par ce terminal esclave C ne pourront pas être désembrouillés car la carte à puce 34 du terminal esclave C comporte un code secret  $S_{S1}$  en relation biunivoque avec le code secret  $S_{M1}$ .

Dans le cas illustré par la figure 2c, le  
 25 code secret maître  $S_{M2}$  transféré dans le terminal esclave D n'est pas compatible avec le code secret  $S_{S1}$  inscrit dans la carte à puce 36. Les programmes embrouillés reçus par le terminal maître A ne pourront pas non plus être reçus par le terminal esclave D.

30 Dans les différents cas, chaque fois qu'un utilisateur veut utiliser un terminal esclave dont le

façon classique au moyen d'un mot de contrôle transmis sous forme chiffré dans un message de contrôle de titre d'accès ECM (pour Entitlement Control Message). Le message ECM est exploité dans le terminal B après avoir  
5 été déchiffré par une clé utilisateur préalablement inscrite dans la carte à puce 32. L'ECM conditionnant l'accès aux programmes est exploitable par le terminal  
10 esclave B du fait que la carte à puce qui lui est associée dispose d'un code secret esclave correspondant de manière biunivoque au code secret maître stocké dans le terminal esclave B.

Ainsi, dans ce cas également, le contrôle des codes secrets de la carte et du terminal peut être effectué indifféremment par la carte ou par le  
15 terminal.

Dans le cas illustré par la figure 2b, le code secret  $S_{M1}$  n'a pas encore été transféré dans le terminal esclave C. Les programmes embrouillés reçus  
20 par ce terminal esclave C ne pourront pas être désembrouillés car la carte à puce 34 du terminal esclave C comporte un code secret  $S_{S1}$  en relation biunivoque avec le code secret  $S_{M1}$ .

Dans le cas illustré par la figure 2c, le code secret maître  $S_{M2}$  transféré dans le terminal  
25 esclave D n'est pas compatible avec le code secret  $S_{S1}$  inscrit dans la carte à puce 36. Les programmes embrouillés reçus par le terminal maître A ne pourront pas non plus être reçus par le terminal esclave D.

30 Dans les différents cas, chaque fois qu'un utilisateur veut utiliser un terminal esclave dont le

code secret maître n'existe pas ou n'est pas compatible avec le code secret de la carte à puce, une annonce s'affiche sur un écran pour l'inviter à insérer la carte à puce associée au terminal maître pour

5 transférer le code secret maître dans le terminal esclave. Le logiciel résident dans la carte à puce ou dans le terminal vérifie la compatibilité des codes secrets maître et esclave et autorise l'utilisation du terminal esclave si ces codes sont compatibles.

10 Il en résulte qu'aucun terminal esclave ne pourra être utilisé sans l'autorisation du terminal maître. Ceci permet d'empêcher la réception frauduleuse de programmes embrouillés par un terminal non muni de droits d'accès.

15

---

REVENDICATIONS

---

1. Procédé de distribution de données et/ou services embrouillés à au moins un terminal maître et à au moins un terminal esclave associé audit terminal maître, procédé caractérisé en ce qu'il comporte les étapes suivantes :

----- transmettre au terminal maître un premier code secret  $S_M$  et au terminal esclave un deuxième code secret  $S_s$  en relation biunivoque avec le premier code  $S_M$ ,

- autoriser la réception des données et/ou services par le terminal esclave uniquement si le premier code secret  $S_M$  est préalablement enregistré dans le terminal esclave.

15

2. Procédé selon la revendication 1 caractérisé en ce qu'il comporte les étapes suivantes :

- définir un premier type de messages de gestion de titres d'accès (EMMm) pour transmettre le premier code secret  $S_M$  au terminal maître, et un deuxième type de messages de gestion de titres d'accès (EMMs) pour transmettre le deuxième code secret  $S_s$  à chaque terminal esclave,

- enregistrer le premier code secret  $S_M$  dans le terminal maître et le deuxième code secret  $S_s$  dans chaque terminal esclave et,

à chaque utilisation d'un terminal esclave,  
- requérir l'enregistrement du premier code secret  $S_M$  dans ledit terminal esclave si ce deuxième code  $S_s$  n'est pas en relation biunivoque avec le code secret  $S_M$  enregistré dans le terminal esclave.

---



3. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une étape consistant à générer à fréquence variable un nouveau code secret  $S_M$  et un nouveau code  $S_S$  en relation biunivoque avec le nouveau code  $S_M$ .

4. Procédé selon la revendication 3 caractérisé en ce qu'il comporte les étapes suivantes :

- 10 - définir un premier type de messages de gestion de titres d'accès (EMMm) pour transmettre le nouveau code secret  $S_M$  au terminal maître, et un deuxième type de messages de gestion de titres d'accès (EMMs) pour transmettre le nouveau code secret  $S_S$  à
- 15 chaque terminal esclave,
- enregistrer ce nouveau code secret  $S_M$  dans le terminal maître et le nouveau code secret  $S_S$  dans chaque terminal esclave et,
- à chaque utilisation d'un terminal esclave,
- 20 - si ce nouveau code secret  $S_S$  n'est pas en relation biunivoque avec le code secret  $S_M$  préalablement enregistré dans le terminal esclave,
- requérir l'enregistrement du nouveau code secret  $S_M$  dans ledit terminal esclave.

25

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que chaque terminal comporte un processeur de sécurité.

~~6. Procédé selon la revendication 5,~~  
caractérisé en ce que le processeur de sécurité est une  
carte à puce associée au terminal.

5                   7. Procédé selon la revendication 6,  
caractérisé en ce que ladite carte à puce est appariée  
audit terminal.

8. Système de distribution de données et/ou  
10 services embrouillés à au moins un terminal maître et à  
au moins un terminal esclave, munis chacun d'un  
processeur de sécurité, ledit système comportant :

- un module central de gestion des abonnés  
(14),

15                   - un générateur de messages de gestion de  
titres d'accès (EMM) (16),

- une plate-forme d'embrouillage (18),  
système caractérisé en ce qu'il comporte en  
outre :

20                   - des moyens pour attribuer à chaque  
terminal maître un premier code secret  $S_M$ , et à chaque  
terminal esclave un deuxième code secret  $S_S$  en relation  
biunivoque avec le premier code secret  $S_M$ ,

- des moyens de contrôle destinés à  
25 autoriser la réception des données et/ou services par  
un terminal esclave uniquement si le premier code  
secret  $S_M$  est préalablement mémorisé dans ledit  
terminal esclave.

9. Système selon la revendication 8, caractérisé qu'il comporte un seul terminal maître et un seul terminal esclave.

5 10. Système selon la revendication 8, caractérisé en ce qu'il comporte une pluralité de terminaux maîtres, et une pluralité de terminaux esclaves.

10

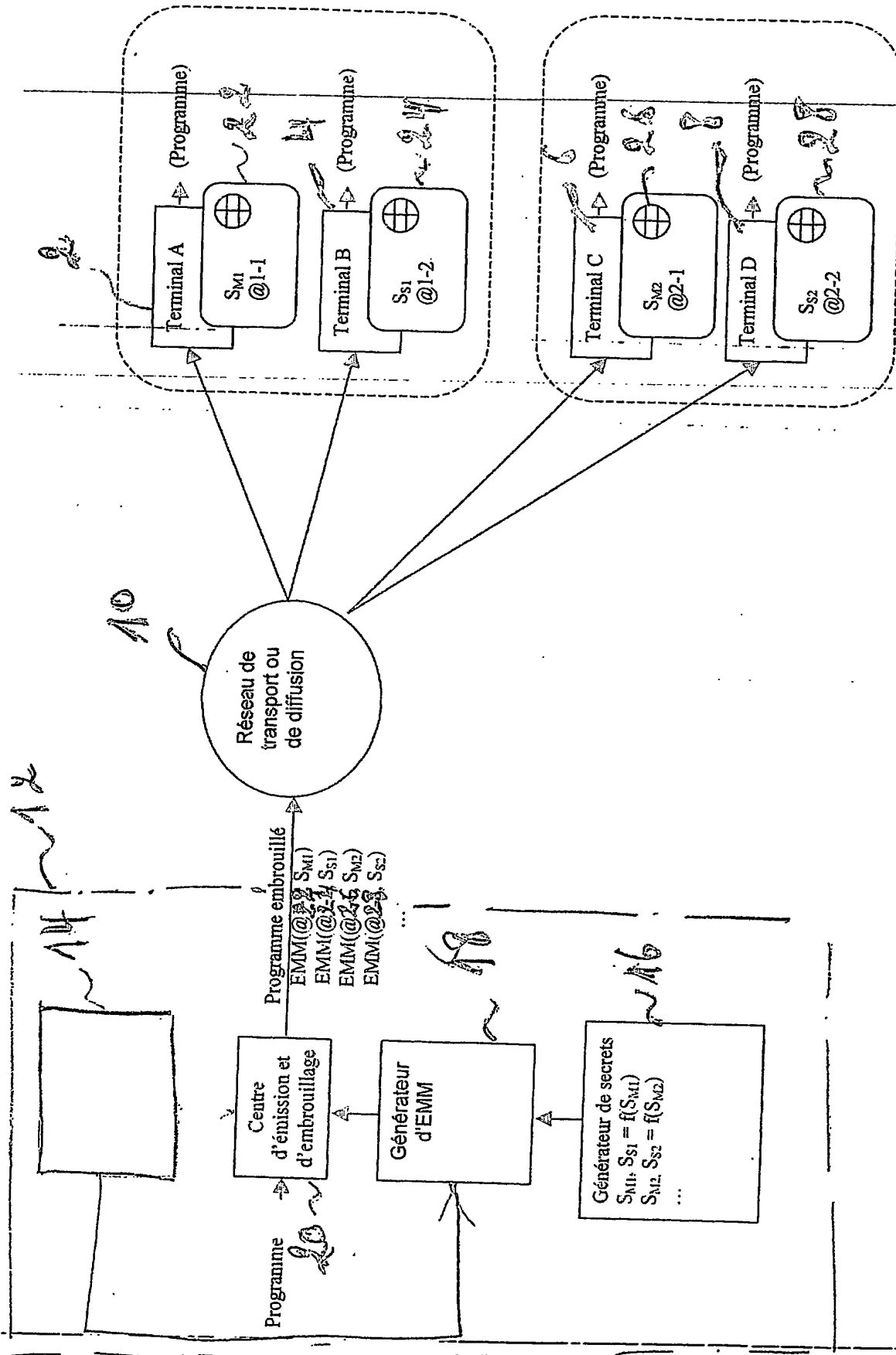


FIG 1

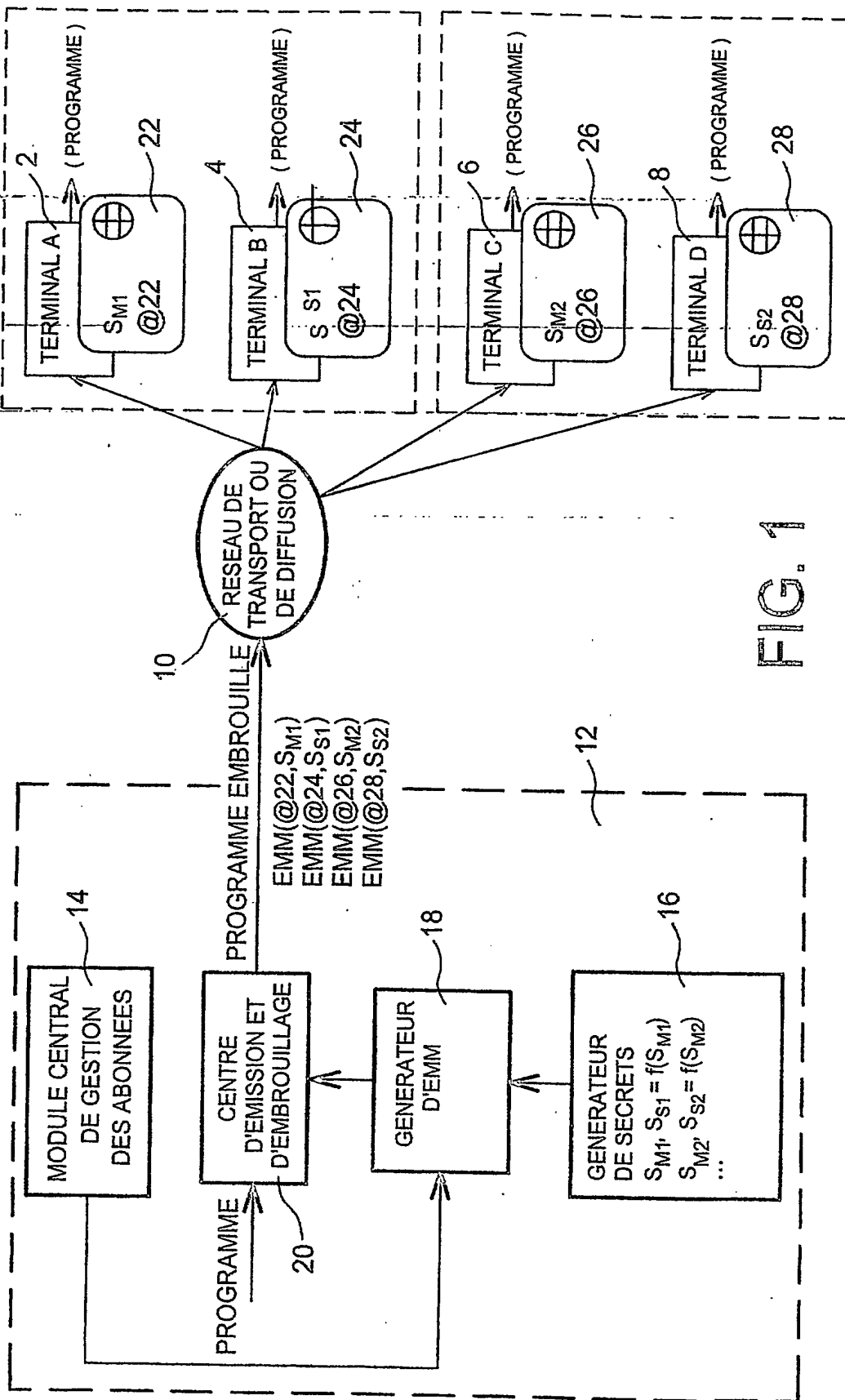
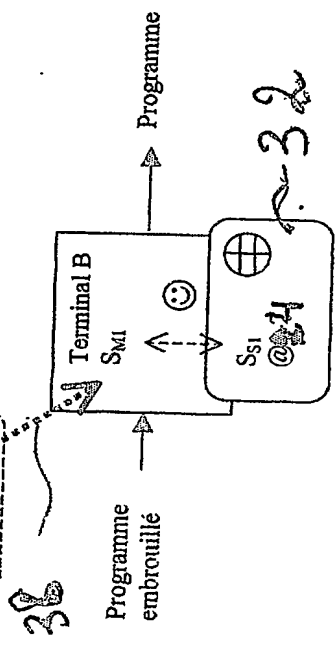
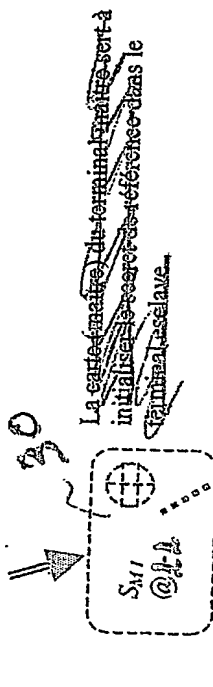
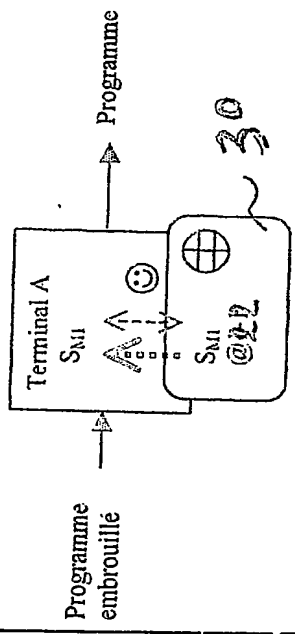


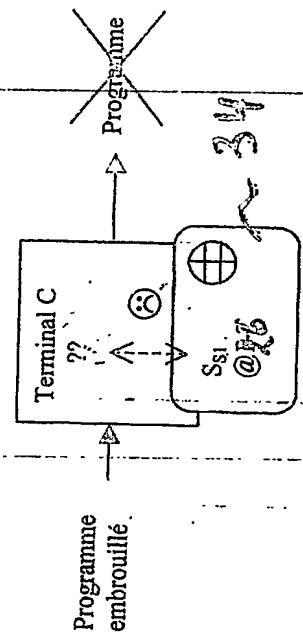
FIG. 1



Terminal disposant d'un secret maître compatible avec le secret esclave de la carte

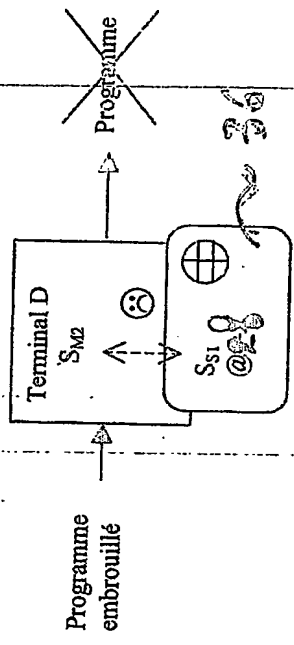
FIG 2a

~~Accès au secret maître présent dans la carte~~



~~Terminal ne disposant pas de secret maître~~

Fig 2b



~~Terminal disposant d'un secret maître non compatible avec le secret esclave de la carte~~

Fig 2

~~Comparaison du secret présent dans la carte à celui présent dans le terminal.~~  
~~2 secrets maîtres, ils doivent être égaux~~  
~~1 secret maître (terminal) et un secret esclave (carte) : ils doivent respecter  $S_s = f(S_M)$~~

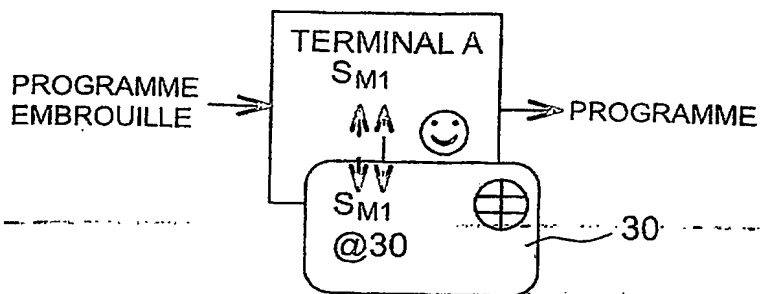


FIG. 2a

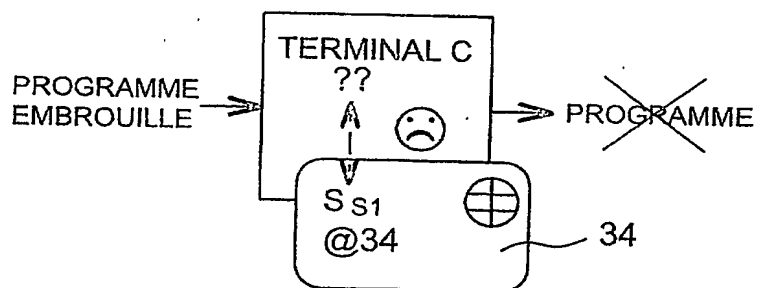
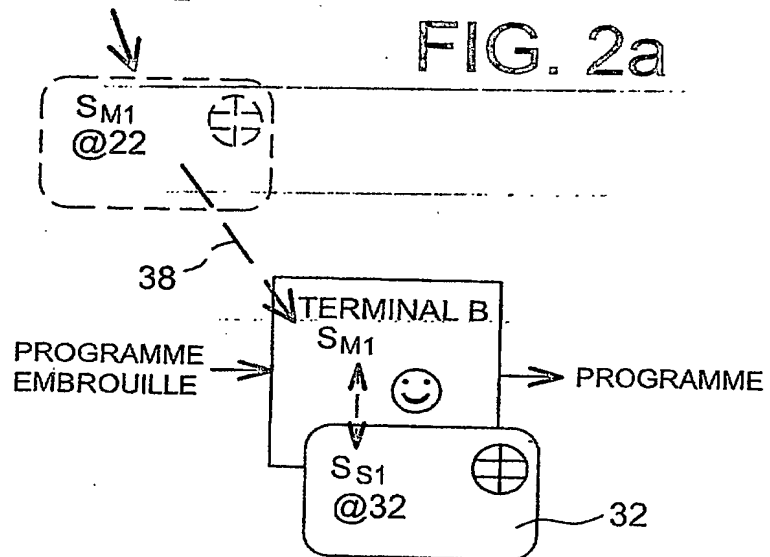


FIG. 2b

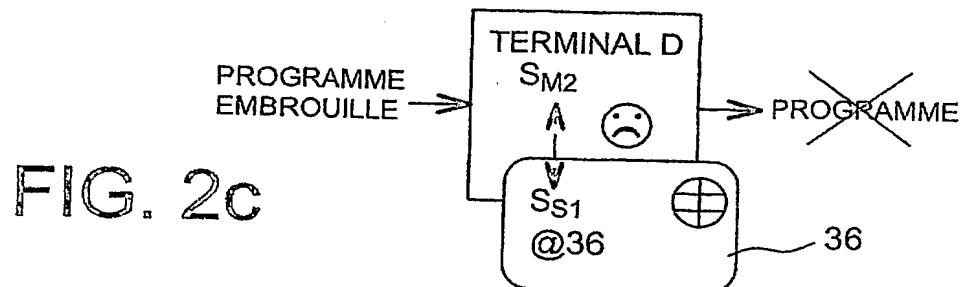


FIG. 2c

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

**DÉSIGNATION D'INVENTEUR(S)** Page N° 1.../1...

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 6 W / 270601

<b>Vos références pour ce dossier (facultatif)</b>	SP 21819/HM
<b>N° D'ENREGISTREMENT NATIONAL</b>	02.15736 DU 12.12.2002.

**TITRE DE L'INVENTION** (200 caractères ou espaces maximum)

PROCEDE DE DISTRIBUTION DE DONNEES ET/OU SERVICES EMBROUILLES.

**LE(S) DEMANDEUR(S) :**

VIACESS  
Les Collines de l'Arche - Tour Opéra C  
92057 PARIS LA DEFENSE CEDEX

**DESIGNE(NT) EN TANT QU'INVENTEUR(S) :**

<b>1</b>	<b>Nom</b>	LE BARS
	<b>Prénoms</b>	Bernard
	<b>Adresse</b>	Rue
		6 Clos Perault
	<b>Code postal et ville</b>	19 1 2 0 0   ATHIS-MONS FRANCE
	<b>Société d'appartenance (facultatif)</b>	
<b>2</b>	<b>Nom</b>	AALST
	<b>Prénoms</b>	Theo Van
	<b>Adresse</b>	Rue
		Sophiastraat 99
	<b>Code postal et ville</b>	15 1 5 8 3   CB WAALRE HOLLANDE
	<b>Société d'appartenance (facultatif)</b>	
<b>3</b>	<b>Nom</b>	
	<b>Prénoms</b>	
	<b>Adresse</b>	Rue
	<b>Code postal et ville</b>	
	<b>Société d'appartenance (facultatif)</b>	

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

**DATE ET SIGNATURE(S)**

**DU (DES) DEMANDEUR(S)**

**OU DU MANDATAIRE**

(Nom et qualité du signataire)

PARIS/LE 9 JANVIER 2003

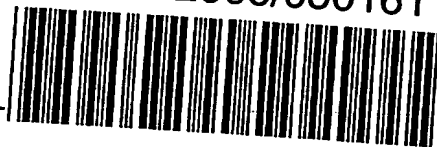
D. DU BOISEAUDRY

CPI 95 304





PCT Application  
PCT/FR2003/050161



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**